[19]中华人民共和国国家知识产权局

Ref 1

[51]Int. Cl[7]
G06F 11/28

[12]发明专利申请公开说明书

[21]申请号 99124432.X

[43]公开日 2001年5月16日

[11]公开号 CN 1295281A

[22]申请日 1999.11.9 [21]申请号 99124432.X

[71]申请人 王 涛
地址 518020 广东省深圳市福田区益田村75栋503室
共同申请人 汪询晔
[72]发明人 王 涛 汪询晔

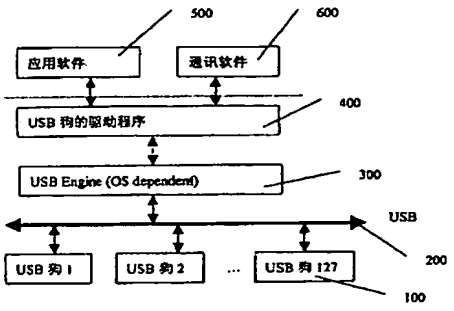
[74]专利代理机构 深圳市顺天达专利商标代理有限公司
代理人 郭伟刚

权利要求书3页 说明书9页 附图页数4页

[54]发明名称 基于通用串行总线接口的软件正版验证方法和装置

[57]摘要

一种基于通用串行总线接口的软件正版验证方法和装置，以通用串行总线为待验证者和授权者的通讯的接口，检测并启动USB狗；在USB狗被启动后由应用程序发送查询码给USB狗；USB狗收到查询码后产生应答码并将该应答码发送给应用程序；应用程序将收到的应答码与计算的应答码比较产生验证结论。这种方法和装置支持热拔插、即插即用、多任务处理和多达127个USB狗的同时使用，安全性好，可靠性高，可广泛应用于各种软件的正版验证。



ISSN1008-4274

权 利 要 求 书

1、一种基于通用串行总线接口的软件正版验证方法，以通用串行总线（USB）为待验证者和授权者的通讯的接口，其特征在于，包括以下步骤：检测并启动 USB 狗；在 USB 狗被启动后由应用程序发送查询码给 USB 狗；USB 狗收到查询码后产生应答码并将该应答码发送给应用程序；应用程序将收到的应答码与计算的应答码比较产生验证结论。

2、根据权利要求 1 所述方法，其特征在于，所述检测并启动 USB 狗包括以下步骤：将 USB 狗插入 PC 的 USB 口中；在操作系统检测到一个新的 USB 设备时，操作系统从已经安装的文件库中查找驱动程序，如果没有找到，则提示用户提供驱动程序安装盘，装好驱动程序；如找到驱动程序后，则启动 USB 设备驱动程序。

3、根据权利要求 1 所述方法，其特征在于，所述在 USB 狗被启动后由应用程序发送查询码给 USB 狗包括以下步骤：应用软件（待验证者）被启动；由该应用程序调用 USB 设备驱动程序的接口，给 USB 狗发送查询码；如果失败，则未获验证，执行非正版的程序逻辑；如果发送成功，驱动程序通过操作系统的应用接口将查询码数据发送到 USB 总线上。

4、根据权利要求 1 所述方法，其特征在于，所述 USB 狗收到查

询码后产生应答码并将该应答码发送给应用程序包括以下步骤：所述 USB 狗接收到查询码后，根据预定算法计算应答码，并将应答码送到 USB 总线；而操作系统的底层软件接受到该应答码数据后传送给 USB 狗的驱动程序；由 USB 狗驱动程序将应答码发送给应用程序。

5、根据权利要求 1 所述方法，其特征在于，所述应用程序将收到的应答码与计算的应答码比较产生验证结论包括以下步骤：应用程序计算预定的应答码，将其与通过 USB 接收到的应答码进行比较，如果不一致，则未获验证，执行非正版的程序逻辑；如果完全一致，则认为自己是合法的，按正版逻辑执行。

6、一种基于通用串行总线接口的软件正版验证装置，其特征在于，包括：用于与 USB 接口连接的接插件 1、与所述接插件 1 连接的串行通讯设备 2、与所述串行通讯设备 2 连接的微处理器核心单元 3，还包括分别与所述微处理器核心单元 3 连接的 I/O 设备单元 4 以及外部存储设备 5，来自所述 USB 接口的信号被所述串行通讯设备（SCU）2 收到并整理成字节并引起所述微处理器核心单元 3 的一个中断，所述微处理器核心单元 3 运行的中断处理程序可将字节形式的数据作为参数，运行预置在所述外部存储设备（EMD）5 中的程序并将计算出结果返回所述微处理器核心单元 3 作为应答码，并通过所述串行通讯设备 2 通过接插件 1 和 USB 传送到主计算机。

7、根据权利要求 6 所述装置，其特征在于，所述微处理器核心单元 3 包括 CPU 以及与 CPU 连接的存储器，所述外部存储设备 EMD

是闪频存储器或 EEPROM，用于存放应用开发方开发的软件加密算法等。

8、根据权利要求 6 所述装置，其特征在于，所述串行通讯设备 SCU2 和所述微处理器核心单元 3 可以包含在一个集成电路中。

9、根据权利要求 8 所述装置，其特征在于，所述集成电路的型号可以是 CY7C63000 系列的 IC。

10、根据权利要求 6 所述装置，其特征在于，所述 I/O 设备单元 4 可以是发光二极管作为显示输出。

99.11.11

说 明 书

基于通用串行总线接口的软件正版验证方法和装置

本发明涉及计算机安全技术，更具体地说，涉及一种基于通用串行总线（USB）接口的软件正版验证方法和装置。

众所周知，盗版软件给软件开发公司带来了巨大的经济损失。软件开发公司除了宣传和鼓励消费者使用正版软件外，还选择使用加密手段来保护自己的知识产权。通过加密，软件产品能够鉴别当前运行的是正版还是非法复制的盗版。下表归纳了现有的主要软件加密方法的分类。

表一：软件加密方法的种类

	安装介质加密	安装过程加密	硬件加密
技术原理	通过对标准设备的额外信息空间进行读写来识别正版	识别产品的序列号，用独特的序列号算法来鉴别正版	读取硬件信息来识别正版软件
识别的时效	安装时、运行时	安装时	安装时、运行时
技术定位	防止最终用户的盗版	防止最终用户的盗版、防止销售渠道的盗版	防止最终用户的盗版、防止销售渠道的盗版
解密方法	使用非常规的拷贝的软件和硬件对额外的数据进行复制	散发安装序号、复制安装后的系统	复制硬件、一带多、虚拟硬件
利弊	简单而成本低、效用低	容易实现、有时可能需要额外的技术支持，效用中等	需要添加硬件可能会带来兼容性问题、费用高、效用高

其中，硬件加密技术相对其他两种技术而言，技术可靠性较高，但需要进一步解决兼容性以及使用方便性等问题。小型的硬件加密设备俗称“软件狗”。其原理举例说明如下，在计算机（PC）的标

准并行端口上加插一个带有预置数据或程序的“软件狗”，在需要验证为正版方能使用的软件产品中，设置一段需要正确读取该软件狗中数据方能运行的程序。如果读取的数据与预期的相同，则验证通过，否则验证不合格，软件将拒绝其进一步运行。

本发明的目的是提供一种新的软件正版验证方法，这种方法可以用来确定运行软件是否具有合法版权，并且可以有效克服现有软件加密技术的诸多缺点，使得这种验证方法具有很强的安全性和使用上的便利和灵活性。

本发明的另一目的是提供一种新的软件正版验证装置，这种装置采用了通用串行总线(USB)为硬件接口,可以克服现有软件加密装置（软件狗）存在的缺点，具有物理上接口新、体积小而且使用方便的特点。为沿袭过去对这种设备的称呼习惯，我们称这种设备为 USB 软件狗，简称 USB 狗。

在说明本发明的方法之前，可将软件和加密设备视为两个具有计算能力的独立主体，且称为待验证者和授权者。假设待验证者和合法的授权者都知晓验证的算法，即加密算法。验证过程包括以下步骤：

1. 待验证者产生查询码，即某些数据的组合，例如产生的时间；
2. 待验证者发送查询码给授权者；
3. 如果发送失败，则未获验证。
4. 授权者加密查询码，生成应答码；
5. 授权者发送应答码给待验证者；

6. 待验证者也根据知道的算法加密查询码，生成的结果数据与应答码比较，如果一致则验证成功，否则是验证失败。

该过程中的核心是加密算法，同简单的返回静态内容的验证方法比较，算法可以千变万化，令盗版者无法通过仿制授权者来复制和出售盗版。另外一个好处是，通过良好的设计，待验证者和授权者的算法部分的工作都由软件开发商来完成，这样减少了透明度，增强了保密性。在实际应用中，软件主体是待验证者，而“软件狗”是授权者。

本发明的第一目的是这样实现的，构造一种基于通用串行总线（USB）接口的软件正版验证方法，以通用串行总线为待验证者与授权者的通讯接口，验证过程包括以下步骤：1)将 USB 狗插入 PC 的 USB 口中，（假设该 PC 具有 USB 插口）；2)操作系统（如：Windows 98）检测到一个新的 USB 设备，操作系统去从已经安装的文件库中查找驱动程序，如果没有找到，则提示用户提供驱动程序安装盘，装好驱动程序。找到驱动程序后，启动驱动程序；3)应用软件（待验证者）启动；4)应用程序调用驱动程序的接口，试图给 USB 狗发送查询码；如果失败，则未获验证，执行非正版的程序逻辑；5)驱动程序通过操作系统的应用接口将查询码数据发送到 USB 总线上；6)USB 狗接受到查询码，根据知道的算法计算应答码，并将应答码送到 USB 总线；7)操作系统的底层软件接受到应答码数据，传送给 USB 狗的驱动程序；8)驱动程序将应答码发送给应用程序；9)应用程序根据查询码计算预期的应答码，并将之与通过 USB 接收到的应

答码进行比较，如果不一致，则未获验证，执行非正版的程序逻辑；如果完全一致，则认为自己是合法的，按正版逻辑执行。

本发明的另一目的是这样实现的，构造一种基于通用串行总线接口的验证装置，可以配合所运行软件，对该软件是否正版进行验证，其特征在于，包括：与 USB 接口连接的接插件 1、与所述接插件 1 连接的串行通讯设备 2、与所述串行通讯设备 2 连接的微处理器核心单元 3，还包括分别与所述微处理器核心单元 3 连接的 I/O 设备单元 4 以及外部存储设备 5，来自所述 USB 接口的信号被所述串行通讯设备（SCU）2 收到并整理成字节并引起所述微处理器核心单元 3 的一个中断，所述微处理器核心单元 3 运行的中断处理程序可将字节形式的数据作为参数，运行预置在所述外部存储设备（EMD）5 中的程序并将计算出结果返回所述微处理器核心单元 3 作为应答码，并通过所述串行通讯设备 2 通过接插件 1 和 USB 传送到主计算机。

在本发明提供的装置中，微处理器核心单元3包括CPU以及与CPU内置的存储器，如 RAM 和 ROM。

在本发明提供的装置中，串行通讯设备 SCU2 和所述微处理器核心单元 3 可以包含在一个集成电路中，例如型号是 CY7C63000 系列的 IC。

在本发明提供的装置中，I/O 设备单元 4 包括发光二极管，用于指示工作状态，外部存储设备 EMD5 是闪频存储器或 EEPROM，用于存放应用开发方开发的软件加密算法等。

实施本发明提供的基于通用串行总线（USB）接口的软件正版验证方法和装置，同现有技术相比，由于接口采用了通用串行总线USB，使得其具有以下显著的特点：1）支持热拔插; 2）支持即插即用; 3）支持多任务处理; 4）支持多达127个USB狗的同时使用。更为重要是，本发明的验证装置由于采用内置单片机的USB控制器，通过固化的软件实时按特制的算法进行校验，所以，具有安全性好，可靠性高的突出优点，能有效地抑制盗版，保护国家利益，保障软件厂家的基本权益。本发明提供的基于USB接口的验证方法和装置可广泛应用于各种软件的正版验证。

结合附图和实施例，进一步说明本发明的特点，附图中：

图1是应用本发明提供验证方法的体系结构示意图；

图2是说明本发明验证方法的流程示意图；

图3是本发明验证装置的原理性说明框图；

图4是说明在实现本发明验证方法中，本发明的验证装置（USB狗）执行的程序流程示意图；

图5是本发明装置的电路原理示意图。

在说明本发明的方法和装置之前，对作为实现本发明基础的通用串行总线（英文全称 Universal Serial Bus，简称 USB）简要说明如下：

USB接口（标准1.0版本）具有以下一些特点：

1） 串行速度达到12Mb/s，超过以太网（10Mb/s）；

2） 基于协议的串行总线管理，采用主从模式，最多可以挂接127

个从属设备；

3） 带电接插外设，自动识别设备的类型和加载驱动程序，真正意义上的即插即用；

4） 灵活的协议支持等时传输模式和异步消息模式；

5） 提供协议扩展空间支持创新的外设类型；

6） 接口统一，简单而且造价低。

本发明的方法和装置，就是在上述 USB 接口的基础上实现软件版权验证和访问合法性验证的。其基本体系结构如图 1 所示，USB 总线 200 上可以连接多达 127 个本发明提供的验证装置 100，这种装置就是 USB 狗。它作为带有 USB 接口计算机的一个外部设备，用以验证运行的软件是否正版。它是一种新型接口的验证设备，采用了国际上正日益兴起的通用串行总线 USB，并符合 IT 产业各大厂家提出的 USB 标准 1.0 版。每个 USB 狗可以独立运行，也可以交互作用，无论哪一种方式，均需要通过与操作系统相关的 USB 引擎 300 连接到 USB 狗的驱动程序模块 400，而被验证的应用程序 500 和被验证的通信程序 600 均通过该驱动程序模块 400、USB 引擎 300、USB 总线 200 与该总线上的某一个（单独作用）或几个（多重作用）USB 狗 100 交互作用实现对软件是否正版的验证。此处，USB 引擎（USB Engine）是指包括软件、硬件在内的一种机制，用于将放送的数据包变成 bit 流，再将之转换为 USB 总线上的电气信号。上述说明其验证原理是这样的：

被验证软件 500 通过 USB 接口 200 向 USB 狗 100 内的微处理器

发送查询码，再由 USB 狗 100 内的微处理器，进行特殊的校验算法处理，返回应答码给被验证软件 500 来检验其是否正版。一种典型的算法是待加密数据与某个特别字符串(俗称密钥)做逻辑异或操作，计算得到查询码。USB 狗 100 得到查询码后，再将查询码与密钥做异或操作，就可以得到原来的待加密数据了。

本发明方法利用 USB 狗进行软件版权验证的步骤如下：

1 启动应用软件；

2 软件检查系统有无 USB 狗；若无，则提示插入硬件；

3 插上 USB 狗；

4 USB 狗加电初始化；

5 软件检测到 USB 狗；

6 软件向 USB 狗发查询码；

7 若无应答码返回，软件进入步骤 2；

8 按照预定的算法检验 USB 狗返回的应答码，若正确，软件进入正常工作状态；若否，软件提示插入正确的 USB 狗，进入步骤 2。

启动被验证的软件，在检查到所述 USB 接口上插有验证装置(USB 狗）时，向所述 USB 狗发查询码并等待 USB 返回应答码，当接收到来自 USB 狗的应答码与预期的相同时，则通过验证，如果没有在规定时间内收到来自 USB 狗的应答码或收到的应答码与预期的不同，则未通过验证。

结合附图 2，对上述利用 USB 狗进行验证的过程说明如下：

如图 2 所示 ，在框 201 中进行程序初始化，在框 202 中，生成随机数作为查询码，在框 203 中，根据查询码计算期望的应答码，在框 204 中，将计算出来的查询码传送给操作系统的 USB 引擎，在框 205 中，由 USB 引擎将查询码传送给 USB 狗，在框 206 中，由 USB 狗根据查询码计算应答码，在框 207 中，由 USB 狗将计算出的应答码传送给 USB 引擎，在框 208 中，比较接收到应答码和在前计算出的期望应答码进行比较，在框 209 中判断两者是否相等，如果相同，则在框 210 中验证成功，如果不相同，则在框 211 中进入验证失败，最后，均在框 212 中结束。其中框 205-207，不属于驱动程序内部功能，而是驱动程序的外部调用。

图 3、图 4 和图 5 分别给出了本发明装置（USB 狗）的硬件逻辑框图和软件流程以及电路原理图。如图 3 所示，验证装置（USB 狗）主要包括外部存储设备（EMD）5、微处理器核心单元 3、串行通讯设备（SCU）2、I/O 设备 4 和通用串行总线（USB）接口 1，其中，外部存储设备（EMD）5 、I/O 设备 4 分别连接到微处理器 MCU 的 I/O 端口，该微处理器核心单元 3 的 I/O 端口还通过串行通讯设备（SCU）2 与通用串行总线 USB 的接口 1 连接。 所述串行通讯设备 SCU2 和所述微处理器核心单元 3 可以包含在一个集成电路，如型号是 CY7C63000 系列的 IC。I/O 设备单元 4 可以是发光二极管 LED 作为显示输出。整个电路逻辑满足 USB 标准 1.0 版。在其具体实现的电路原理图（图 5）中，D-数据线用 7.5K 精密电阻上拉到 VCC，采用 USB 标准 1.0 版规定的 1.5M 低速传输模式。使用时，当系统

加电，LED1 灯亮；USB 狗初始化，正常工作后，LED2 灯同时点亮。工作时来自所述 USB 接口的信号被所述串行通讯设备（SCU）2 收到并整理成字节并引起所述微处理器核心单元 3 的一个中断，所述微处理器核心单元 3 运行的中断处理程序可将字节形式的数据作为参数，运行预置在所述外部存储设备（EMD）5 中的程序并将计算出结果返回所述微处理器核心单元 3 作为应答码，并通过所述串行通讯设备 2 通过接插件 1 和 USB 传送到主计算机。具体过程如图 4 所示，在框 401 中，加电开始，在框 402 中，对寄存器进行初始化，在框 403，初始化中断向量，在框 404 中，查询有无 USB 通讯中断，如无回到框 404 继续等待有无中断发生，如有 USB 通讯中断，则在框 405 中，取得来自计算机主机（PC）的查询码，在框 406 中，运行在外部存储设备中的程序，根据查询码计算出应答码（变形码），最后在框 407 中，将应答码通过串行通讯单元 2、USB 接口发送到主计算机中，完成正在主机上运行的软件有无合法版权。

采用了本发明的基于 USB 接口的软件狗，由于支持热拔插、动态分配资源、允许多个设备共存等特点，较好地解决了上述问题，具有其他硬件加密手段所不可比拟的优越性。

说明书附图

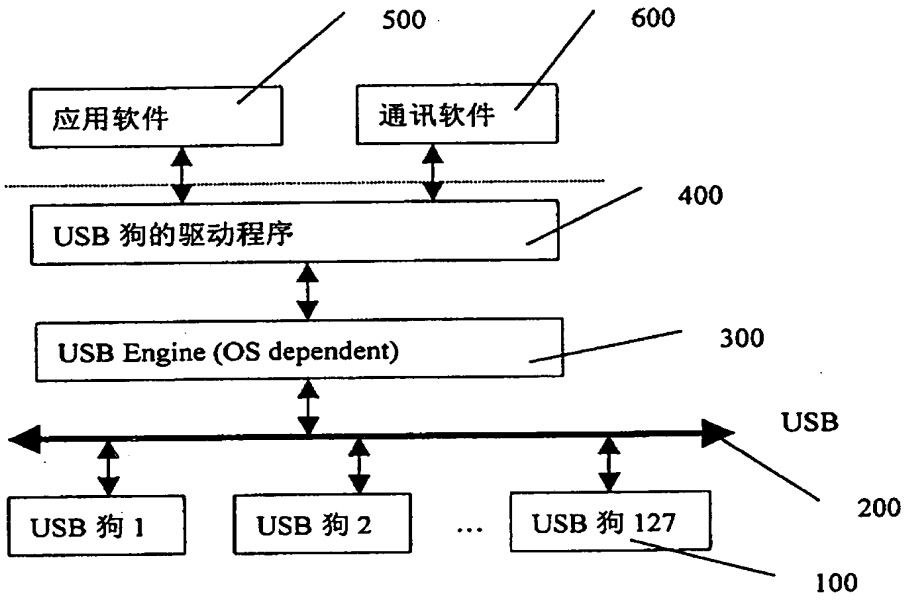

500
600
应用软件
通讯软件
400
USB 狗的驱动程序
USB Engine (OS dependent)
300
USB
200
USB 狗 1
USB 狗 2
...
USB 狗 127
100

图 1

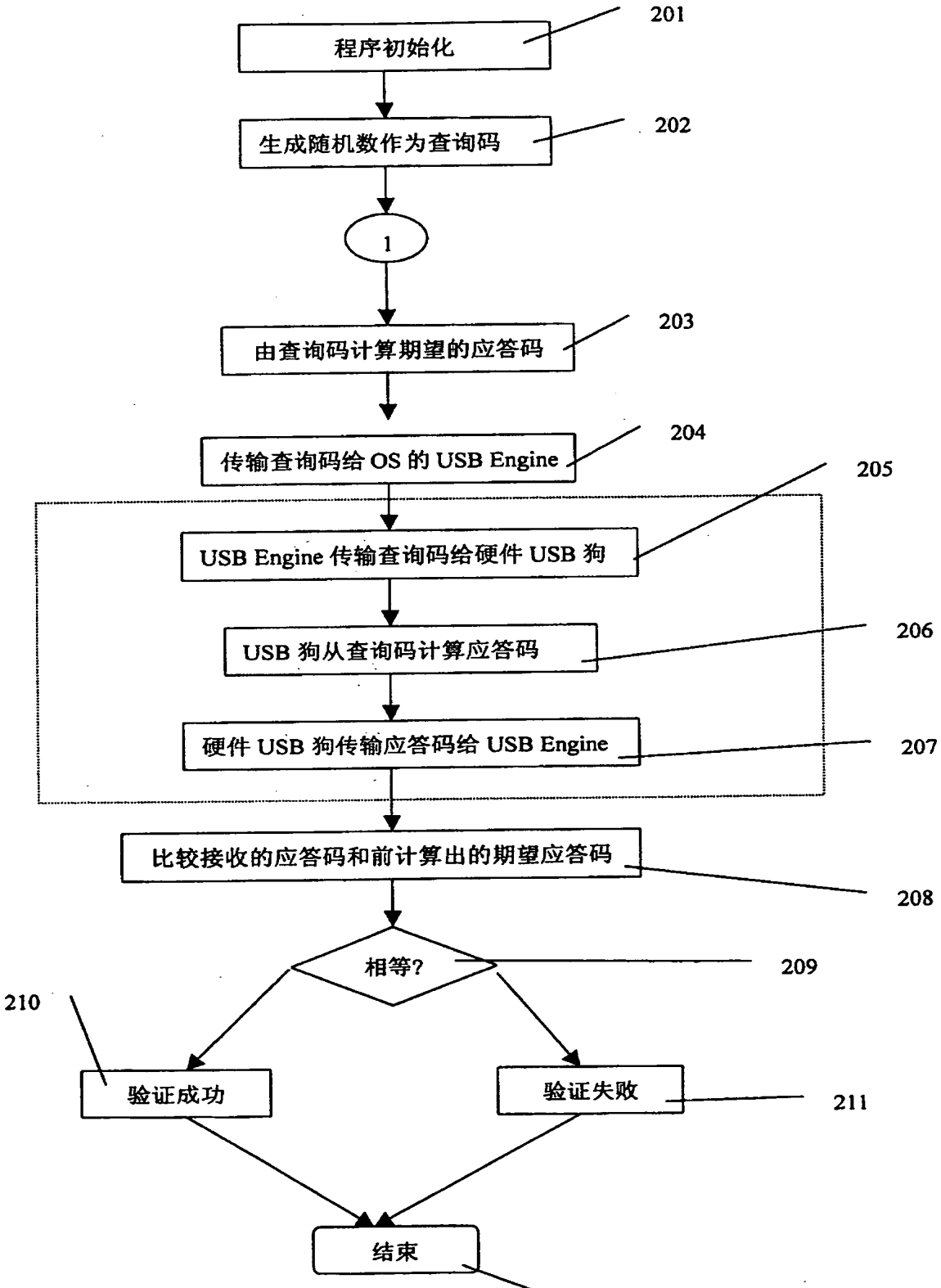

201
程序初始化
202
生成随机数作为查询码
1
203
由查询码计算期望的应答码
204
传输查询码给 OS 的 USB Engine
205
USB Engine 传输查询码给硬件 USB 狗
206
USB 狗从查询码计算应答码
207
硬件 USB 狗传输应答码给 USB Engine
比较接收的应答码和前计算出的期望应答码
208
相等?
209
210
验证成功
验证失败
211
结束
212

图 2

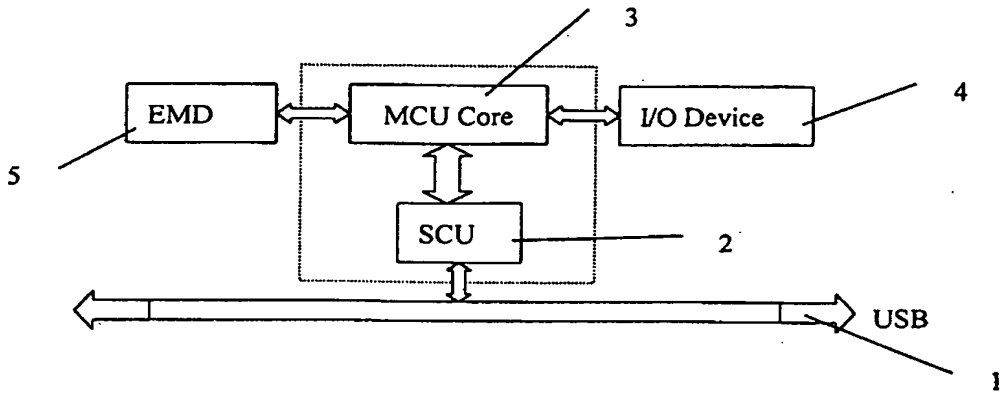

3
EMD
MCU Core
I/O Device
4
5
SCU
2
USB
1

图 3

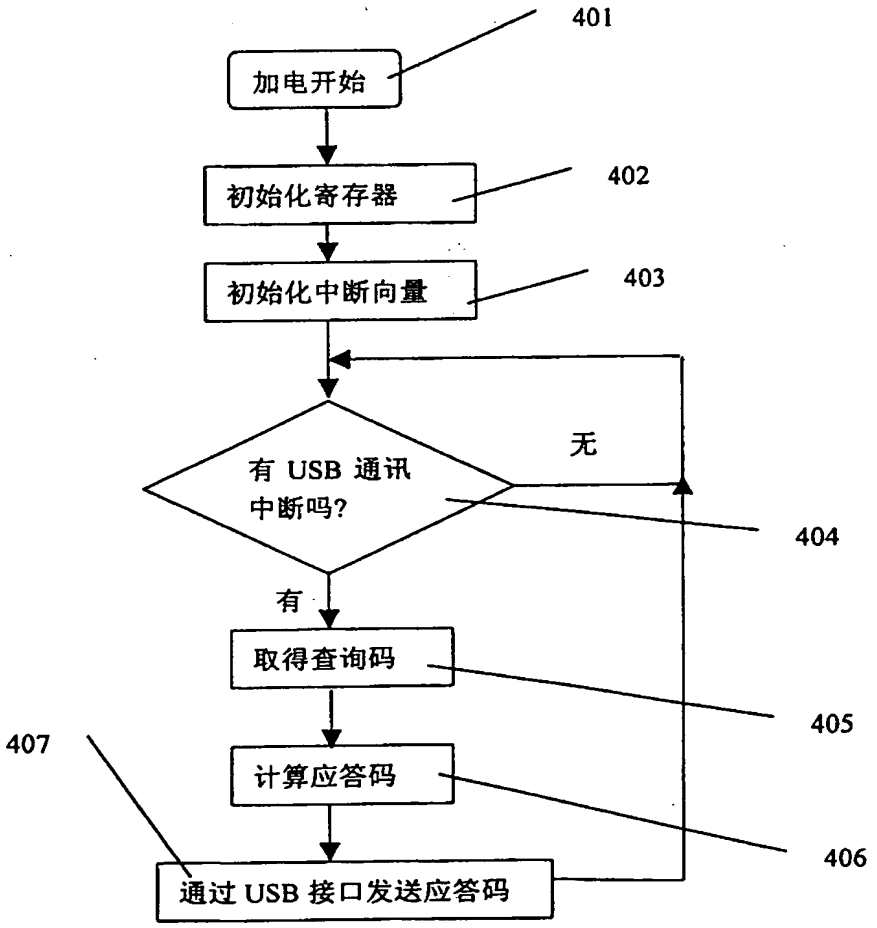

401
加电开始
初始化寄存器
402
初始化中断向量
403
有 USB 通讯
中断吗?
无
404
有
取得查询码
405
407
计算应答码
406
通过 USB 接口发送应答码

图 4

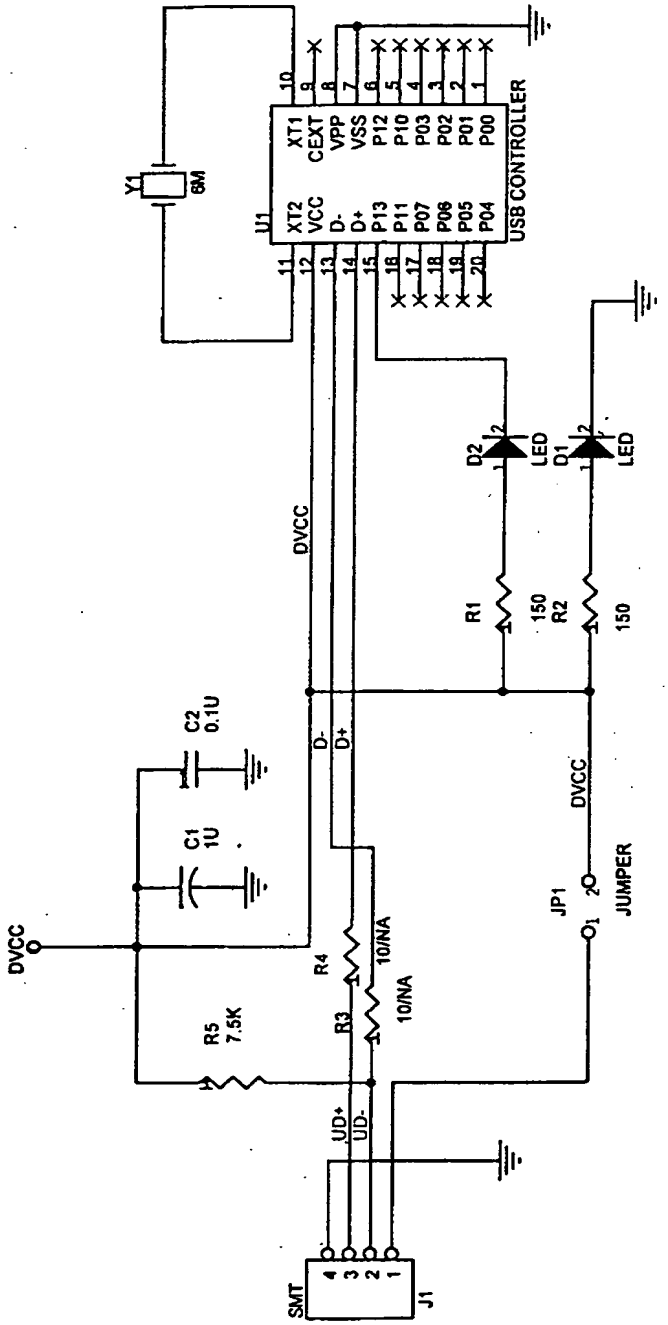

U1
USB CONTROLLER
XT1
CEXT
VPP
VSS
P12
P10
P03
P02
P01
P00
XT2
VCC
D-
D+
P13
P11
P07
P06
P05
P04
X1
6M
D2
LED
D1
LED
DVCC
R1
150
R2
150
C2
0.1U
C1
1U
D-
D+
DVCC
JP1
JUMPER
DVCC
R4
10/NA
R3
10/NA
R5
7.5K
UD+
UD-
SMT
J1

图5

CN 1295281A

SOFTWARE COPYRIGHT AUTHENTICATION METHOD AND APPARATUS BASED ON UNIVERSAL SERIAL BUS INTERFACE

Abstract

A software copyright authentication method and apparatus based on a universal serial bus (USB) interface, in which the universal serial bus interface is used as a communication interface between an authenticated party and an authenticating party, and a USB watchdog is detected and enabled; after the USB watchdog is enabled, an inquiry code is sent to the USB watchdog by an application program; the application program generates an authentication conclusion by comparing a received response code with a calculated response code. The present method and apparatus support hot plug, plug & play, multi-task processing and parallel usage of up to 127 USB watchdogs, and have superior security and reliability, and can be widely used for various software copyright authentication.